SF-SHERLOCK®

I SUOI OBIETTIVI

MASSIMA SICUREZZA
MASSIMA QUALITÀ SU TUTTA
LA PIATTAFORMA Z
TRAMITE AUTOMAZIONE
CON LA MINIMA SPESA

PROTEZIONE TECNICA
E CONFORMITÀ LEGALE
ATTRAVERSO IL COMPLETO
MONITORAGGIO IN
TEMPO REALE

« UNA DELLE PIÙ IMPORTANTI INNOVAZIONI IN AMBITO DI SICUREZZA DEL MAINFRAME DOPO RACF. »

COMPLETO MONITORAGGIO DI SICUREZZA ED ALTA QUALITÀ SULLA PIATTAFORMA Z

Lei è consapevole dei rischi e pericoli odierni, e ritiene quindi di estrema importanza la massima sicurezza informatica per proteggere le principali attività dell'azienda? Nell'era di Internet e dell'E-commerce vuole continuare ad avere fiducia nell'idea «mainframe = massima sicurezza»?

Lei conosce le attuali rigide normative e requisiti legali, come Basilea II, il Manuale di Protezione IT (Ufficio Federale Tedesco per la Sicurezza Informatica), Sarbanes Oxley (SOX), U.S. DOD, Gramm Leach Bliley Act (GLBA), KonTraG, RS FAIT 1, HIPAA, la direttiva 95/46/EC sulla protezione dei dati personali etc., e inoltre le norme di certificazione secondo ISO 17799 e BS 7799? Questi standard richiedono alla Sua azienda precise ed efficaci misure di sicurezza per proteggere tutti i sistemi informatici e i relativi audit trails, inclusa la tecnologia sottostante, da attacchi interni ed esterni. **Lei deve inoltre avere prove evidenti per clienti, azionisti e legali**, che dimostrino che sia stato fatto tutto il possibile, e dal punto di vista tecnico e da quello legale, per garantire i più elevati standard di sicurezza e qualità – e ciò anche nell'intento di ottenere **un buon rating [dei rischi]**. L'obiettivo per il mainframe della Sua azienda è soddisfare tutte queste esigenze tecniche e legali con la minima spesa. Ciò significa ricercare una soluzione completa che lavori automaticamente, altamente efficace a livello tecnico, approvata legalmente e sicura a livello di auditing.

Lei considera sicurezza, qualità ed economia dei costi, fattori di estrema importanza per la competitività? Sa bene che soltanto con il miglioramento della qualità e con il più alto livello di automazione nei processi del lavoro quotidiano, può raggiungere l'ambita produttività migliore. Infine, ciò Le dà anche la flessibilità e il tempo necessari ad affrontare le sfide del commercio odierno e a sfruttare le opportunità del futuro.

Lei vuole una soluzione unica che svolga tutte le operazioni necessarie, come monitorare gli eventi ed esaminare le aree deboli del Suo sistema, attraverso una constante valutazione della sua vulnerabilità, che arrivi davvero a coprire **tutto il campo di azione della piattaforma di mainframe**? E allo stesso tempo, nel Suo livello ideale di valore aggiunto, questa soluzione dovrebbe consentire l'impiego quotidiano e la cooperazione di tutte le diverse aree, vale a dire **dal livello tecnico fino a quello di gestione più elevato**?

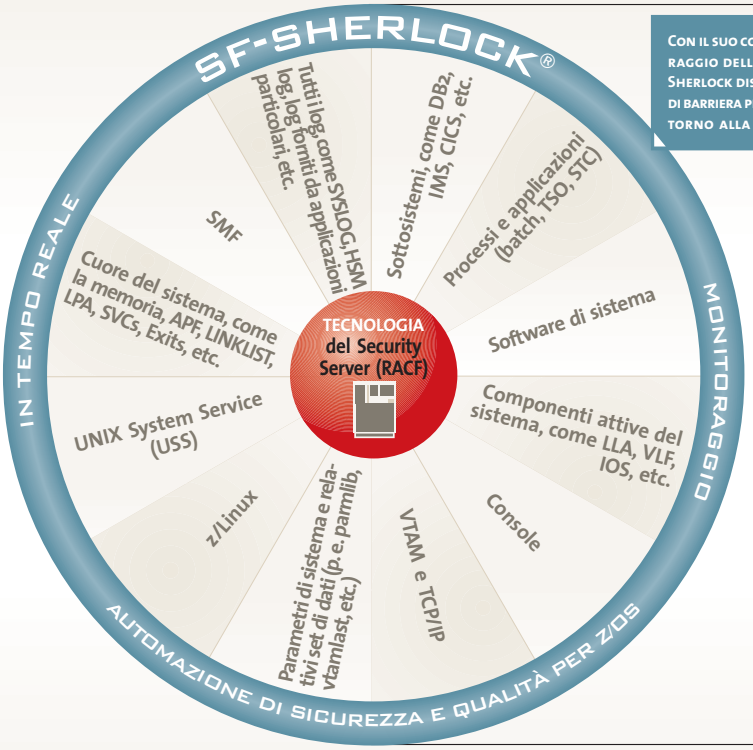
Lei richiede anche la possibilità di integrazione con soluzioni su scala aziendale, per la gestione della sicurezza in cross platform e per l'auditing, e vorrebbe non avere mai dubbi sui Suoi investimenti in queste aree? La soluzione a cui aspira dovrebbe appoggiare i Suoi interessi in modo assolutamente flessibile, anche nell'ambito di **ITIL, COBIT e BS 7799**, tra gli altri?

AUTOMAZIONE DELLA SICUREZZA E DELLA QUALITÀ Z CON SF-SHERLOCK È LA RISPOSTA AI NUOVI CAMPI DELL'APPLICAZIONE Z NELL'ERA DI INTERNET E DELL'E-BUSINESS

PRESTAZIONI

- PROTEZIONE 24 ORE SU 24 TRAMITE MONITORAGGIO IN TEMPO REALE
- MONITORAGGIO DELLE APPLICAZIONI
- ALLEGGERIMENTO DEL LAVORO E RIDUZIONE DEI COSTI
- TOTALE GARANZIA DI QUALITÀ
- RIVELAMENTO DI FURTI DI AUTORIZZAZIONI E PRIVILEGI COSÌ COME DI QUALUNQUE MANIPOLAZIONE (DINAMICA) DEL PROTOCOLLO, DELLE FUNZIONI LOG, DELLA MEMORIA, ETC.
- RIVELAMENTO DI ATTIVITÀ ED EVENTI SOSPETTI COME AD ESEMPIO LE FUGHE DI DATI ATTRAVERSO LE COSIDDETTE «TRAPPOLE LOGICHE»
- NOTIFICAZIONI E REAZIONI AUTOMATICHE
- CONTROLLO E AUDITING LEGALMENTE CONFORMI
- MONITORAGGIO DI FILE CON DELTA REPORTING
- MONITORAGGIO DI INTRUSIONI ESTERNE ED INTERNE
- RILEVAMENTO DI INTRUSI E DI FUGHE DI DATI
- CONFORMITÀ CON GLI STANDARD LEGALI COME SOX, KONTRAG, ISO, BS, U.S. DOD, UFFICIO FEDERALE TEDESCO PER LA SICUREZZA INFORMATICA (BSI), ETC.
- IMPORTANTE SOSTEGNO PER TUTTI I REPARTI DELL'AZIENDA
- REPORTING COMPRENSIVO DI PUNTEGGI
- CONSENTE LA CONNESSIONE CON QUALSIASI TICKET, PROBLEM ED ALTRI SISTEMI DI GENERE ITIL
- CAPACITÀ DI FARE RAPPORTO SULLA SPECIFICA DI CLIENT
- PROTEZIONE E DIFESA CONTRO ABUSI E MANOMISSIONI
- INTERFACCE ACCESSIBILI CHE CONSENTONO DI INTERAGIRE FACILMENTE
- COSTANTE TEST DI PENETRAZIONE SIMULATA, PRIVO DI CONTROINDICAZIONI, PER UNA VALUTAZIONE COSTANTE DELLA VULNERABILITÀ
- ESAME DI QUALITÀ DELLE PASSWORD
- CONSENTE L'INCAPSULAMENTO DELLE APPLICAZIONI COME POTENTE MISURA DI SICUREZZA CONTRO ATTACCHI QUALI AD ESEMPIO BUFFER OVERFLOW E FORMAT STRING
- SUPPORTA OGNI GENERE DI SORGENTE DI DATI, COME SMF, LOG, ETC.
- PROVVISTO DI POLICIES COMPLETE
- RISULTATI SICURI A LIVELLO DI AUDITING (LOG, REPORT, ETC.)
- SIMULAZIONE (AD ESEMPIO IPL)
- ESAMI DI SINTASSI E DI SEMANTICA DEI FILE DI SISTEMA (PARMLIB, VTAMLST, ETC.)
- OPERAZIONE TOTALMENTE AUTOMATIZZATA
- I DISPOSITIVI DI CONNESSIONE CONSENTONO UNA FACILE INTEGRAZIONE IN SOLUZIONI DI SICUREZZA PER CROSS PLATFORM E DI GESTIONE DEL SISTEMA, COME SYMANTEC, CA, TIVOLI, ETC.

Dr. Stephen Fedtke
ENTERPRISE-IT-SECURITY.COM



CON IL SUO COMPLETO MONITORAGGIO DELLA SICUREZZA, SF-SHERLOCK DISPONE UNA SORTA DI BARRIERA PROTETTIVA TUTT'ATTORNO ALLA PIATTAFORMA Z.

IMPRESA

- **Policies e normative legali**
- **Notificazione e reazione automatiche**
- **Logging sicuro a livello di auditing**
- **Connessione e integrazione**
- **Reporting**
- **...**

SOLUZIONE: SF-SHERLOCK, MONITORAGGIO IN TEMPO REALE DI SICUREZZA E QUALITÀ

»Tecnologia: SF-Sherlock rappresenta l'elevata prestazione della **tecnologia di monitoraggio in tempo reale, per la realizzazione di un'automazione di sicurezza e qualità complete** sulla piattaforma z attraverso l'integrazione di monitoraggio, registrazione, notificazione, reazione, reporting, e delle possibilità di simulazione (per esempio IPL) in una soluzione completa. Con i suoi componenti, SF-Sherlock è un processo di sistema costantemente attivo che monitora ed esamina la sicurezza del sistema (server di sicurezza o RACF, o anche CA-TSS e CA-ACF2), i processi specifici e i sottosistemi (DB2, LDAP, etc.), così come il sistema operativo z/OS in tutte le sue componenti. Esso registra i cambiamenti rilevanti in un modo sicuro a livello di auditing, quindi informa tempestivamente e dettagliatamente la persona addetta sugli eventi dell'area interessata, come errori, attacchi, manipolazioni, cambiamenti, etc., ad esempio con una E-mail o un SMS. Conformemente a quanto detto, il reparto di auditing ottiene monitoraggio e valutazioni continuamente automatizzati, inclusivi di reporting. Ciò significa che nessuno deve elaborare manualmente i dati e perdere tempo con compiti di routine, dato che tutti i processi sono completamente automatizzati. **Ciò Le concede libertà, flessibilità e sicurezza**. SF-Sherlock va oltre il puro reporting in casi ben definiti. Per esempio, con la sua funzione opzionale di reazione automatica e istantanea, SF-Sherlock caccia immediatamente fuori del sistema gli intrusi. Con il suo controllo e la sua sorveglianza costanti, nel senso di una protezione **24 ore su 24**, Lei ottiene il necessario livello massimo di sicurezza e di qualità, che Le fa prendere potere sul Suo sistema, riducendo inoltre i costi.

»La necessità di agire non può essere negata: Fin dal 2004 l'Ufficio Federale Tedesco per la Sicurezza Informatica (BSI) è andato ben oltre il livello del Dipartimento di Difesa degli Stati Uniti (U.S. DOD), discutendo apertamente dei rischi e definendo le misure di sicurezza necessarie per la piattaforma di mainframe z/OS nella sua essenziale guida della sicurezza, il «Manuale di Protezione IT». Il messaggio-chiave esprime la necessità di **«utilizzare un monitoraggio della sicurezza in tempo reale per i sistemi z/OS onde poter rilevare più velocemente le violazioni della sicurezza»**. Un monitoraggio in tempo reale soltanto di un singolo ed isolato aspetto della sicurezza, quale garantiscono, ad esempio, le registrazioni SMF, non è ancora sufficiente. Monitorare l'intero z/OS in tutte le sue componenti, nella complessità dei suoi nessi e dei dettagli, è indispensabile. SF-Sherlock monitora il sistema z/OS completamente e approfonditamente, poiché il principale pericolo proviene da procedure «a trabocchetto» non rilevate, e da errori nascosti ovunque in z/OS, operate col fine, ad esempio, di ottenere importanti autorizzazioni, di danneggiare l'audit trail o di raggiungere accessi non rilevati alle risorse. In questo modo dei professionisti possono spiare tutti i dati, attraverso aggiramenti ben calcolati e manipolazioni della sicurezza del sistema, senza lasciare neppure una singola registrazione SMF o log. In conseguenza di ciò, qualunque erroneo parametro o configurazione di sistema rimasto nascosto potrebbe mettere in pericolo la validità dell'intero sistema, al più tardi col prossimo IPL. Sia le carenze di sicurezza sia quelle di qualità portano ugualmente a delle catastrofi, e devono quindi essere entrambe prevenute «ad ogni costo». Per questo, dopo ogni modifica operata nel sistema, **SF-Sherlock controlla automaticamente la sicurezza del Suo sistema, come ad esempio le parmlib e altri importanti file di sistema, per ogni possibile mancanza o errore**. Una tecnologia in tempo reale è necessaria perché il tempo di durata per manipolazioni da parte di attività illegali professionistiche è estremamente breve – il rilevamento, la prevenzione attraverso una reazione tempestiva, la presentazione di prove consistenti, non sono possibili in altro modo. La checklist di possibili vulnerabilità ed errori è ampia e può essere effettuata solo da un monitoraggio completamente automatizzato.

»Tecnologia che garantisce risultato: Garantendo sicurezza e qualità automatiche e complete, la tecnologia di SF-Sherlock raggiunge appieno i notevoli obiettivi sopra menzionati, rendendo la Sua piattaforma di mainframe conforme a tutte le diverse normative e requisiti legali. Con SF-Sherlock, Lei non solo soddisfa esigenze irrinunciabili, ma ottiene inoltre, **sia totale garanzia di qualità, sia protezione assoluta**. SF-Sherlock blinda la strada verso il futuro della Sua impresa. Monitoraggio ed esami costanti e completi, soprattutto ai livelli tecnici più profondi, stanno diventando sempre più importanti con le nuove funzioni di z/OS (Unix System Service, Sysplex Technology, etc.) e con le nuove aree di applicazione, come web server, data server e piattaforme di E-commerce. Non ci sono quindi dubbi che le misure di sicurezza standard si riveleranno col tempo sempre più insufficienti. La funzione di **SF-Sherlock quale sistema di rilevamento di intrusioni e di fughe, per la difesa contro attacchi interni ed esterni**, è ancora più significativa in quanto rappresenta il più alto livello di protezione contro la crescente apertura verso l'esterno di sistemi e di network in precedenza chiusi. Con la sua tecnologia leader, SF-Sherlock è un essenziale passo nel raggiungimento di un livello costante e moderno di sicurezza e qualità per combattere questi rischi.

»Produttività che garantisce successo: Essendo un processo automatico che agisce in tempo reale, SF-Sherlock lavora per i reparti di gestione della sicurezza e di auditing, per quelli di protezione dei dati e delle informazioni e per quelli della tecnologia del sistema. Inoltre, esso li integra in un unico workflow altamente efficiente, che conduce **ad una più elevata produttività e ad una significativa riduzione dei costi**. Attraverso la sua completa automazione di sicurezza e qualità, SF-Sherlock è una soluzione integrata per tutta l'azienda, anche in contesti di cross platform. Il suo valore aggiunto assicura la più alta redditività e convenienza di prezzi per tutte le parti in questione. Con il concetto di implementazione «plug and play», Lei raggiunge questo obiettivo e le conseguenti prestazioni, nonché la conformità legale, con il minimo dispendio di tempo e denaro.